WinZip Unquoted Path Vulnerability

Found by: Christopher Iwen aka Strat0m
Date: 12/17/2020
Software Name: WinZip
Site: https://www.winzip.com/win/en/
Download Link: https://download.winzip.com/gl/nkln/winzip25-home.exe
Downloaded: winzip25-home.exe
File size: 955 KB
Tested on: Windows 10 pro 64-bit

When installing WinZip I chose the evaluation copy. There were no issues during the install process. After installing WinZip, the WZUpdateNotifier.exe started calling C:\program.exe on each reboot. It was doing this as the user that is logged into the system at that time, which can be a significant security vulnerability depending on that users permissions. The big security vulnerability is during the uninstall of WinZip. The uninstall calls C:\program.exe a total of 5 times each as the user "nt authority\system" which means it has full control of the system.

This vulnerability means that an attacker could place a malicious file named program.exe in the C:\ folder and wait for WinZip or the uninstaller to call it. This would initiate the malicious executable with the same permissions being used to run the software and could be used to do anything from installing malicious software to opening a reverse shell.

This flaw exists because of how Windows searches for programs that contain a space in the name. For instance when trying to call C:\Program Files (x86)\Some Program\run.exe without any quotes, Windows will do so in this order:

C:\Program.exe
C:\Program Files.exe
C:\Program Files (x86)\Some.exe
C:\Program Files (x86)\Some Program\run.exe

Fortunately the fix for this is very simple. The software in question just needs to have quotes put around each of those paths it is calling. So instead of calling C:\Program Files (x86)\Some Program\run.exe it should be calling "C:\Program Files (x86)\Some Program\run.exe".

This flaw was found using a program I created. You can see the output of the program and the screenshots in the notes below. The source code and explanation for program.exe can be found at https://github.com/ciwen3/Public/tree/master/C%2B%2B/Unquoted-Path-Vuln

On Start Up:
Program.exe was run on each start up as the currently logged in user with the following privilege:

Privilege Name	Description	State
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled

When checking what process ran the command that ended up calling program.exe during the startup it showed as the same process on each start up, "C:\Program Files\WinZip\WZUpdateNotifier.exe" -show. Which was running the following command:

C:\Program Files\WinZip\WZUpdateNotifier.exe -showOnly -allowParallelExecution -productcode="WZC" -buildid="0" -version="25.0.14273.0" -language="en" -uid="8b77febc-5481e7ab-5c37bf83-506df074" -puid="8b77febc-5481e7ab-5c37bf83-506df074" -checkType="scheduled" -dsi="0" -apps="WZC" -cpN1="winzipInfo/productOriginID" -cpV1="nkln" -cpT1=string -cpN2="winzipInfo/productVendorID" -cpV2="nkln" -cpT2=string -cpN3="winzipInfo/productState" -cpV3="0" -cpT3=number -cpN4="winzipInfo/licenseHolder" -cpV4="" -cpT4=string -cpN5="winzipInfo/licenseKey" -cpV5="" -cpT5=string

During Uninstall:

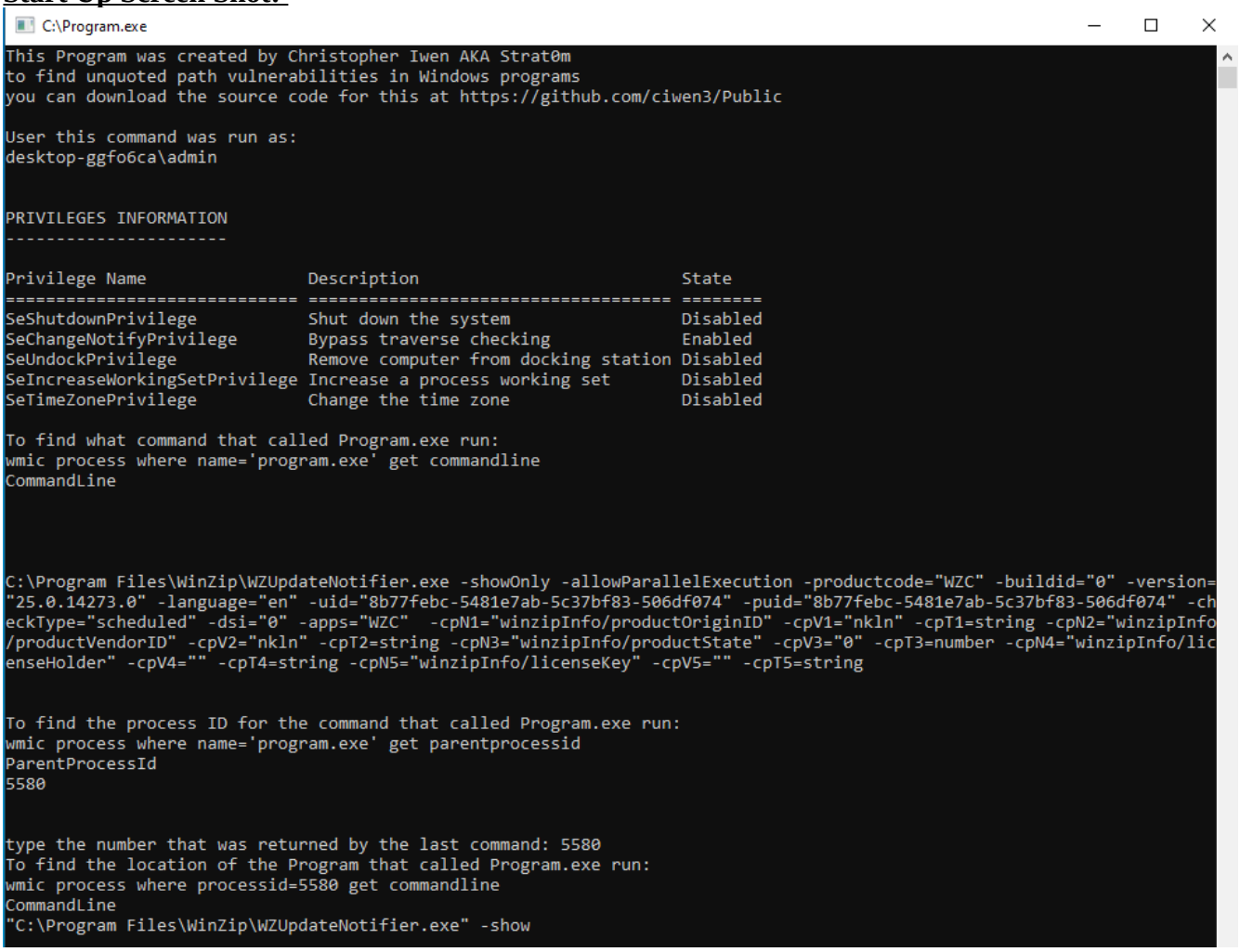
Program.exe was run all 5 times as “nt authority\system” with the following privileges:

Privilege Name	Description	State
SeLockMemoryPrivilege	Lock pages in memory	Enabled
SeTcbPrivilege	Act as part of the operating system	Enabled
SeSecurityPrivilege	Manage auditing and security log	Enabled
SeProfileSingleProcessPrivilege	Profile single process	Enabled
SeIncreaseBasePriorityPrivilege	Increase scheduling priority	Enabled
SeCreatePagefilePrivilege	Create a pagefile	Enabled
SeCreatePermanentPrivilege	Create permanent shared objects	Enabled
SeAuditPrivilege	Generate security audits	Enabled
SeChangeNotifyPrivilege	Bypass traverse checking	Enabled
SeImpersonatePrivilege	Impersonate a client after authentication	Enabled
SeCreateGlobalPrivilege	Create global objects	Enabled
SeCreateSymbolicLinkPrivilege	Create symbolic links	Enabled

When checking what process ran the commands that ended up calling program.exe during the uninstall it showed as the same process all 5 times, C:\Windows\system32\msiexec.exe /V. Which was running the following commands:

1. C:\Program Files\WinZip\WzPreviewer64.exe -stop
2. C:\Program Files\WinZip\WzCABCacheSyncHelper64.exe /u
3. C:\Program Files\WinZip\WzPreloader.exe stop
4. C:\Program Files\WinZip\WzBGTComServer64.exe /UNREGSERVER
5. C:\Program Files\WinZip\WzBGTools64.exe /u

Start Up Screen Shot:



Uninstall Screenshots:

```
User this command was run as:
nt authority\system


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeAuditPrivilege                Generate security audits                  Enabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled

To find what command that called Program.exe run:
wmic process where name='program.exe' get commandline
CommandLine
C:\Program Files\WinZip\WzPreviewer64.exe -stop


To find the process ID for the command that called Program.exe run:
wmic process where name='program.exe' get parentprocessid
ParentProcessId
3044


type the number that was returned by the last command: 3044
To find the location of the Program that called Program.exe run:
wmic process where processid=3044 get commandline
CommandLine
C:\Windows\system32\msiexec.exe /V
```

```
User this command was run as:
nt authority\system


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeAuditPrivilege                Generate security audits                  Enabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled

To find what command that called Program.exe run:
wmic process where name='program.exe' get commandline
CommandLine
C:\Program Files\WinZip\WzCABCacheSyncHelper64.exe /u


To find the process ID for the command that called Program.exe run:
wmic process where name='program.exe' get parentprocessid
ParentProcessId
3044


type the number that was returned by the last command: 3044
To find the location of the Program that called Program.exe run:
wmic process where processid=3044 get commandline
CommandLine
C:\Windows\system32\msiexec.exe /V
```

```
User this command was run as:
nt authority\system


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeAuditPrivilege                Generate security audits                  Enabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled

To find what command that called Program.exe run:
wmic process where name='program.exe' get commandline
CommandLine
C:\Program Files\WinZip\WzPreloader.exe stop


To find the process ID for the command that called Program.exe run:
wmic process where name='program.exe' get parentprocessid
ParentProcessId
3044


type the number that was returned by the last command: 3044
To find the location of the Program that called Program.exe run:
wmic process where processid=3044 get commandline
CommandLine
C:\Windows\system32\msiexec.exe /V
```

```
User this command was run as:
nt authority\system


PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                               State
============================= ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeAuditPrivilege                Generate security audits                  Enabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled

To find what command that called Program.exe run:
wmic process where name='program.exe' get commandline
CommandLine
C:\Program Files\WinZip\WzBGTComServer64.exe /UNREGSERVER


To find the process ID for the command that called Program.exe run:
wmic process where name='program.exe' get parentprocessid
ParentProcessId
3044


type the number that was returned by the last command: 3044
To find the location of the Program that called Program.exe run:
wmic process where processid=3044 get commandline
CommandLine
C:\Windows\system32\msiexec.exe /V
```

```
User this command was run as:
nt authority\system


PRIVILEGES INFORMATION
----------------------

Privilege Name                  Description                               State
=============================== ========================================= ========
SeAssignPrimaryTokenPrivilege   Replace a process level token             Disabled
SeLockMemoryPrivilege           Lock pages in memory                      Enabled
SeIncreaseQuotaPrivilege        Adjust memory quotas for a process        Disabled
SeTcbPrivilege                  Act as part of the operating system       Enabled
SeSecurityPrivilege             Manage auditing and security log          Enabled
SeTakeOwnershipPrivilege        Take ownership of files or other objects  Disabled
SeLoadDriverPrivilege           Load and unload device drivers            Disabled
SeProfileSingleProcessPrivilege Profile single process                    Enabled
SeIncreaseBasePriorityPrivilege Increase scheduling priority              Enabled
SeCreatePagefilePrivilege       Create a pagefile                         Enabled
SeCreatePermanentPrivilege      Create permanent shared objects           Enabled
SeBackupPrivilege               Back up files and directories             Disabled
SeRestorePrivilege              Restore files and directories             Disabled
SeShutdownPrivilege             Shut down the system                      Disabled
SeAuditPrivilege                Generate security audits                  Enabled
SeChangeNotifyPrivilege         Bypass traverse checking                  Enabled
SeImpersonatePrivilege          Impersonate a client after authentication Enabled
SeCreateGlobalPrivilege         Create global objects                     Enabled
SeCreateSymbolicLinkPrivilege   Create symbolic links                     Enabled

To find what command that called Program.exe run:
wmic process where name='program.exe' get commandline
CommandLine
C:\Program Files\WinZip\WzBGTools64.exe /u


To find the process ID for the command that called Program.exe run:
wmic process where name='program.exe' get parentprocessid
ParentProcessId
3044


type the number that was returned by the last command: 3044
To find the location of the Program that called Program.exe run:
wmic process where processid=3044 get commandline
CommandLine
C:\Windows\system32\msiexec.exe /V
```